Notice of Allowability	Application No.	Applicant(s)	
	09/327,477	KURODA ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *23 September 2004*.

2. ☒ The allowed claim(s) is/are *1-10,12-19 and 22-26*.

3. ☒ The drawings filed on *08 June 1999* are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 09/23/04
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Allowable Subject Matter

1. This communication is in response to the information disclosure statement (IDS) received on September 23, 2004.

2. Claims 1-10, 12-19 and 22-26 are allowed.

3. The following is an examiner's statement of reasons for allowance:

The above-mentioned IDS lists an European office action for application No. 99304647.3 that introduces the following references:

Menezes, Oorschot, Vanstone, 'Handbook of applied cryptography', CRC press, 1997, pages 4-5 and 551-553.

The primary reasons for the allowance of the independent claims 1, 15-17 and 22-24 are the inclusion of the following limitations that are not found in the prior art listed above and they are uniquely distinct features. Menezes et al teaches the purpose and techniques of cryptography. Menezes et al also teaches various techniques for distributing secret keys. Menezes et al fails to anticipate or render the following limitations:

"Claim 1: a key management unit managing an individual key unique to said electronic data storage apparatus to which said management unit belongs, and a common key shared with other electronic data storage apparatuses of the group, selecting the individual key when performing an encryption process on an electronic document stored in said electronic data storage apparatus to which said management unit belongs, and selecting the common key when performing the encryption process or when verifying the electronic document transmitted to or received from another electronic data storage apparatus; and

an encryption unit performing the encryption process using the key selected by said key management unit."

"Claim 15: re-encrypting, by a first electronic data storage apparatus in one hierarchical level of the hierarchical structure, a document encrypted using an individual key which is unique to and stored in the apparatus, using a higher order group key corresponding to the hierarchical level, and transmitting the re-encrypted document to an electronic data storage and management apparatus for managing the electronic data storage apparatuses in a group at one hierarchical level lower;

verifying, by said electronic data storage and management apparatus for managing a lower group of electronic data storage apparatuses, the received document using the higher order group key, re-encrypting the received document using the lower order group key corresponding to one hierarchical level lower if the received documents

is correct as a result of the verification, and transmitting the received document to a second electronic data storage apparatus in the group at one level lower; and

verifying, by the second electronic data storage apparatus, the received documents using the lower order group key, re-encrypting the received document using an individual key unique to the second electronic data storage apparatus if the electronic document is correct as a result of the verification, and storing the re-encrypted received document."

"Claim 16: re-encrypting, by a first electronic data storage apparatus in one hierarchical level of the hierarchical structure, a document encrypted using an individual key which is unique to and stored in the apparatus, using a lower order group key corresponding to the hierarchical level, and transmitting the re-encrypted document to a lower order group electronic data storage and management apparatus for managing the electronic data storage apparatuses in the group;

verifying, by said electronic data storage and management apparatus for managing a lower group of electronic data storage apparatuses, the received document using the lower order group key, re-encrypting the received document using the higher order group key corresponding to one hierarchical level higher if the electronic document is correct as a result of the verification, and transmitting the document to a receiving electronic data storage apparatus in the group at one level higher; and

verifying, by the receiving second electronic data storage apparatus, the received document using the lower order group key, re-encrypting the received document using

an individual key unique to the second electronic data storage apparatus if the electronic document is correct as a result of the verification, and storing the re-encrypted received document."

"Claims 17 and 23: storing in a storage unit an individual key unique to an electronic data storage apparatus for storing an electronic document and a common key shared with another electronic data storage apparatus;

selecting the common key stored in the storage unit as a key to be used when communicating the electronic document;

selecting the individual key to be used when performing an encryption process on the document to be stored in said electronic data storage apparatus; and

performing the communication process or encryption process using the selected key."

"Claim 22: key management means for managing an individual key unique to an electronic data storage apparatus to which said key management means belongs, and a common key shared with other electronic data storage apparatuses, selecting the individual key when performing an encryption process on the electronic document stored in the electronic data storage apparatus to which said means belongs, and selecting the common key when performing an encryption process or when verifying the electronic document transmitted to or received from another electronic data storage apparatus; and

encryption means performing the encryption process using the key selected by said key management unit."

"Claim 24: storing a local encryption key for the local environment locally and storing a global key for the global environment;

receiving a document to be transmitted along with an environment indicator indicating the environment of the document transmission;

selecting one of the local and global encryption keys responsive to the indicator;

encrypting the document with the selected one of the keys; and

transmitting the encrypted document, and

wherein the local key is used for data storage in a local data storage unit only by a local data storage system that stores the local key.

4. The dependent claims 2-10, 12-14, 18,19, 25 and 26 are allowed because they were originally found to include a unique feature not found in the closest abovementioned art.

5. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Abdulhakim Nobahar, Examiner, Art Unit 2132

A.N.

February 21, 2005

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100